Fuzzy Similarity Measures Approach in Benchmarking Taxonomies of Threats against SMEs in Developing Economies

Yeboah-Boateng, Ezer Osei

Published in:
Canadian Journal on Computing in Mathematics, Natural Sciences, Engineering and Medicine

Publication date:
2013

Document Version
Early version, also known as pre-print

Fuzzy Similarity Measures Approach in Benchmarking Taxonomies of Threats against SMEs in Developing Economies

Ezer Osei Yeboah-Boateng

Abstract — *There are various threats that militate against SMEs in developing economies. However, most SMEs fall on the conservative "TV News Effect" of most-publicized cyber-threats or incidences, with disproportionate mitigation measures. This paper endeavors to establish a taxonomy of threat agents to fill in the void. Various fuzzy similarity measures based on multi-attribute decision-making techniques have been employed in the evaluation. The taxonomy offers a panoramic view of cyber-threats in assessing mission-critical assets, and serves as a benchmark for initiating appropriate mitigation strategies. SMEs in developing economies were strategically interviewed for their expert opinions on various business and security metrics. The study established that natural disasters, which are perennial in most developing economies, are the most critical cyber-threat agent, whilst social engineering is the least critical threat.* [1]

Key Words — Fuzzy Similarity Measures, Threats, Vulnerabilities, Cyber-Risks, Taxonomy, Benchmarking.

I. INTRODUCTION

This paper estimates a taxonomy of threat agents which confronts SMEs in developing economies, by using fuzzy similarity measures for multi-attribute decision-making (MADM) techniques.

The taxonomy defines a set of threat agents organized in the order of most likely or critical to the less likely or minor for the threat agents. The taxonomy provides a benchmark of cyber-security challenges by which SMEs can mitigate risks in their systems and networks.

This benchmark offers a common platform about SMEs assets importance or criticality labels that ought to be appropriately safeguarded.

SMEs constitute the majority of businesses in most economies; so the extent and severity of cyber-threats could have dire consequences on the adoption and provisioning of many ICT services and products. Though, the potential of cyber-risks to SMEs could be catastrophic, there is little or no literature or documentation on the vulnerabilities and threats to SMEs [1]. Obviously, a better appreciation of cyber-security challenges with SMEs could ensure secured businesses and avoid the pitfalls associated with "unwanted business risks" [1].

It must be noted that accurately identifying critical assets can lead to proactive detective and preventive measures that eventually mitigates the susceptibility of the vulnerabilities and thus, curtail the impending threats against the SME assets.

Also, the threat agents taxonomy provides panoramic view of the extent and severity of threats militating against SMEs assets and resources. It can also assist in the appropriate determination and formulation of mitigation strategies and policies for the SMEs.

Based on an empirical study on cyber-security challenges confronting SMEs in developing economies, a set of mission-critical assets were analyzed vis-à-vis the extent and severity of cyber-threats, the following threat agents taxonomy is enlisted:

- {Natural disasters > Poor authentication > Viruses (Malwares) > Hacking > No Backup > Spywares (Adwares) > Power failure > Un-scanned attachments > Spam > Social engineering} [2]

1.1. Multi-Attribute Decision-Making (MADM)

Basic decision making problems that face many SMEs are made in view of uncertainties such as cost, outcome and associated implications, etc. SMEs usually have a number of possible decision choices or options, and an array of possible outcomes to choose from [3].

In day-to-day business settings, managers and operatives are confronted with numerous decision scenarios where some managers may differ in decision choices based on their "perceptions, attitudes, motivations and personalities" [4]. It is also not uncommon to have managers or operatives, heretofore referred to as "experts[2]" [5] to have divergent views. In all cases a common denominator is defined, such as a cumulative or aggregated expert opinion or judgment that becomes representative of the group of experts. The aggregates are usually weighted based on various parameters ranging from educational background, experience in specified fields, management, responsibility or ethics, etc.

Due to the uncertainties in business decision making, many probabilistic assessments render the decision model less

[1] Ezer O. Yeboah-Boateng is a Ph.D. Fellow with the center for Communications, Media & Information technologies (CMI), department of Electronic Systems, at Aalborg University in Copenhagen, Denmark. (e-mail: ezer@es.aau.dk or ezer@cmi.aau.dk).

[2] Bilal Ayyub [5] defines an expert as "a very skillful person who [has] had much training and has knowledge in a specialized field".

effective, unless the intrinsic attributes or vagueness are taken into consideration. On the other hand, fuzzy based possibilistic assessment is capable of handling the vagueness and imprecision in the linguistic decision choices [6] [7] [4].

The notion of threat agents assessment is complex and has lots of uncertainties. So any strategy or solution to assess cyber-risk with probability is like avoiding risk complexities and uncertainty measures [2], and instead render the probabilistic risk assessment model "a process that attempts to guess rather than formally predict the future on the basis of statistical evidence" [8].

Even though probabilistic assessment is said to be based on sound mathematical theory of probability, it undoubtedly uses some subjective and qualitative guesstimates [9]. Shaurette [9] posited that these qualitative risk values may be appropriately estimated based on rules, such as fuzzy inference rules, that capture the "consensus" opinions of cyber-security experts.

In this paper, fuzzy similarity measures are used in evaluating the extent and severity of the threats against important or critical assets. The fuzzy multi-attribute decision-making (MADM) based taxonomy on threat agents seeks to motivate SMEs to proactively analyze the various imperative factors critical to the security and business operations. This multifaceted assessment is fraught with subjective considerations and uncertainties.

1.1.1. Taxonomy

Taxonomy from its roots in Greek means method of arrangement. In academia, it is often used in defining the arrangements or order in which groups in sample populations fall in place. It is also used in grouping elements with certain characteristics or attributes and usually ranked based on the unique characteristics of interest.

1.1.2. Benchmarking

Benchmarking is a process of comparing an organization's business or security metrics with individual or sectorial best practices. In cyber-security, the metrics or constructs of interest are dimensioned in terms of susceptibility, reliability, resilience and the ability to continue business operations even in the event of cyber incidents.

Benchmarking connotes the notion of comparing a measured or observed construct with a standard construct assumed to be one of the best measured or observed, in accordance with one's industry standards. Typically, the standardized constructs aid in operational or strategic improvement and efficiency. In cyber-security, the object of benchmarking is to facilitate proactive risk mitigation and to avoid certain pitfalls experienced by some industry practitioners. Strategically, it promotes effective and efficient risk identification and assessment, as well as overall risk management.

1.2.SMEs in Developing Economies

SMEs in developing economies are characterized by low and uncertain revenues [10]. Information systems projects in developing economies are characterized by socio-economic changes or transformations, as well as knowledge transfer and improved skillset to the SMEs. Walsham & Sahay [11] examined various literatures on information systems research in developing economies, and underscored their relevance. The emergence of Internet facilities in developing economies have impacted positively on societies and organizations , especially in areas of connection costs, access speeds and end-users utilization [12].

Ellefsen & von Solms [12] posited that developing economies are, in many instances, overwhelmed by the massive and rapid improvements of the emerging technologies in ICTs. For instance, most SMEs do not have any programs in place to harness the increased bandwidth, with its attendant vulnerability challenges confronting their systems and their customers. SMEs in developing economies are said to have unique challenges, and so "direct" importation of existing ICT solutions from the developed economies may not necessarily address the issues effectively [12].

Developing economies have embraced the emergence of ICT technologies to promote their development agenda and to present new opportunities for economic empowerment of its citizenry. In an ITU organized forum in December, 2011, the panelists underscored the need for developing economies to be pragmatic about cyber-security risks, stressing the criticality to emerging economies [13].

ITU-T [14] in the "Guide to Cyber-security for Developing Countries" alludes to the common areas of cyber-security solutions amongst nation states, but concedes that developing economies have peculiar challenges, requiring customized solutions. In view of the above, this empirical study is geared to assist SMEs in developing economies with threat agents taxonomy based on simple but intuitive fuzzy similarity measures.

1.2.1. Security Challenges with SMEs

SMEs are conceptually characterized as that firm, which are small in size in comparison to large or multi-national corporations [15]. SMEs are usually typified by the following characteristics [15]:

- SMEs have centralized management;
- SMEs have a low level of labor specialization;
- SMEs have simple, informal, direct internal and external information systems; and
- SMEs have intuitive, implicit and short-term strategy.

The concept of engaging external resources for information systems management raises some challenges. Today's management information systems are typified by ensuring that data and all corporate assets are properly safeguarded. Though, most SMEs may outsource that important component of its business, some may resort to using internal resources which are usually not up-to-speed with most security developments in order to save cost.

Julien's [15] concept of simple external information systems whereby the owner-director is supposed to be in total control of all operations may not be the case in today's cyber-economies. SMEs today, though still small in size relatively, are connected with the rest of the world via the Internet. They may have websites which could have its own vulnerabilities. Customers and vendors, as well as some mobile workers, may log-in remotely, all posing some security challenges to the SMEs.

Contributing to Julien's concepts, [16] posits that "the means of obtaining information are a group of interpersonal and informal relationships which are non-institutionalized and unstructured". Again, SMEs today have established structured and standardized forms of communications and information gathering, such as the use of emails. Invoices and tender documents are submitted via email or web portals, meetings are held via Skype, formal and informal communications take place via Instant Messengers (IMs), etc. As long as important business communications take place via the electronic media, the confidentiality of the information or data must be protected, the integrity must be ensured, and that the channels must be available whenever needed [2]. Any breach or compromise of any of these security concerns are the motivations for this research.

Pierre [17] in examining cyber-crime activities indicated that "many SMEs do not consider themselves as having data that is of interest to cyber-criminals and quite often dismiss the need for properly addressing vulnerabilities in their infrastructure". He continued that "the opposite is true; every business today collects data on employees, customers and vendors that are of interest to cyber-criminals".

Whereas cyber-security vulnerabilities pose serious concerns to all businesses, SMEs are usually hard hit victims and find it very difficult to recover after a cyber-attack. Invariably, SMEs are easier targets than large corporations. Large corporations have, in recent times, strengthened their security systems, either as a response to the increased threats or in compliance with regulations.

Globalization and the advancement in Internet technologies have incited SMEs into positioning themselves from small regional based companies to become global, cross-border companies. SMEs are seizing the opportunities offered by globalization to gain access to strategic markets. Whereas, these trends come with many more opportunities for SMEs, they also pose some risks; - the cyber-threats aspects of which are the focus of this study.

Sharma et al [18] provide an overview of the cyber-attacks which prospective customers of e-commerce are likely to encounter while carrying out transactions over the web. They provide a detailed account of highly specialized attacks that are aimed at SMEs. Rapid diffusion of e-commerce and a rising number of interconnected networks have resulted in an escalation of security threats [19].

1.2.2. SMEs Security: Impact on Business Operations

Though SMEs have been persuaded into moving with the information based bandwagon, incidentally, these opportunities have their corresponding challenges that threaten the SMEs, especially cyber-security related issues of confidentiality, integrity and availability (CIA) vulnerabilities, as those weaknesses are exploited by threat agents. The resultant adverse effects or impacts on SMEs are seen as revenue losses, resources depletion, and loss of customer and investor confidence, etc. [2].

Risk is seen as the possibility for loss of confidentiality, integrity and availability due to a specific threat [20]. Typically, cyber-security objective is to deter, prevent, detect, recover from, and respond to threats in cyberspace. Cyber-security is to safeguard the information assets, the information systems and networks that deliver the information, from damage or compromise resulting from failures of confidentiality, integrity and availability [2]. Cyber-security infrastructure is multifaceted and it includes information technology, procedures and practices, laws and regulations, people and organizations; these areas are said to be interrelated and impact each other [21].

1.3. Key Issues

Organizations all over the world are confronted with cyber-security breaches with significant costs associated, such as loss of corporate image or reputation, lost businesses and legal fees [22]. This cost become more profound when SMEs are involved, and especially so, when they are located in developing or emerging economies.

Often, SMEs are attempted to consider themselves as not having any data that are of interest to any threat agents; that is, they are not susceptible to attacks [17]. On the contrary, every business in today's cyber-economies has data that can serve as attack vectors to the criminal hackers (crackers) or threat agents, in general. For example, employees or customer data, or some intellectual properties are usually highly sought after information.

The issue is what are some of the threat agents that often militate against SMEs in developing economies? What are the more probable threats that are likely to impact significantly on the SMEs? What are the extent of impact on the SMEs should these threats mature?

By identifying threat agents in a frequently updated taxonomy, SMEs can consistently benchmark with most probable threats to their assets [23]. This sort of identification is geared towards effective risk management as possible consequences can be evaluated and appropriate risk mitigation measures proffered proactively [8].

Generally, there's lack of standardized lists of threat agents and their attributes. In modeling human threat agents, [23] alluded to the prevalent "TV News Effect" of most-publicized threats with disproportionate mitigation measures. This deficit of "aggregated, consistent, state-of-the-art" threat agents

hamper with effective risk management efforts [23]. This paper is, thus, motivated in establishing the taxonomy of threat agents amongst SMEs in developing economies as step in creating standardized threat agents, which can serve as benchmarks . This is intended to facilitate the building of secured organizations across developing economies.

1.4. Methodology

This paper is a subset of a broader cyber-security vulnerabilities study on SMEs in developing economies. Cognizant of the complexities and uncertainties in cyber-security metrics, the study set off with extensive literature review and designed a survey questionnaire philosophy which was submitted to five (5) cyber-security practitioners for review and comments [2] [24]. Based on their comments and advice, a pre-test survey was designed and administered to these experts, again for critique. The actual full scale survey was then launched and administered using LimeSurvey Online (www.limesurvey.com) facilities. This approach was adopted in order to target most SMEs in Ghana and Nigeria; and in view of the challenges associated with physically distributing questionnaires in the case-study countries. *To ensure credible results, a cookie was set-up in the online survey program to prevent repeated participation* [2].

The objective of this paper is to create taxonomy of most common threat agents that are most likely to impact on SMEs in developing economies. ICT-based SMEs, financial organizations and government agencies were target samples, and they were selected by a simple random sampling. For instance, the lists of Ghana ISPs Association (GISPA), Nigerian Internet Exchange (NIX) Association and professional IT experts in Ghana and Nigeria were used [2].

Research Approach

In this study, a set of objective-based questionnaire was administered to about 500 SMEs in Ghana and Nigeria, via email messages and a hypertext link to a web portal where the actual survey was administered and processed [2].

The questionnaire had four (4) categories, namely business profile, security posture, cyber-assets classification and possibility of occurrences [2]. From the cyber-assets sub-section, a number of critical assets were evaluated. Six (6) mission-critical assets deduced from the study were DNS server, Email server, Routers, Database server, Core Switches and Web servers [2], according to the SMEs in developing economies.

Also, from the possibility of occurrences sub-section, a number of threat agents were identified as paramount. Based on the above, another web-based survey (under the auspices of www.surveygizmo.com) was administered to 20 randomly selected cyber-security experts for their opinions. Fourteen (14) out of the 20 respondents were received and those constitute the datasets [2] for this paper.

There was a preamble to the email with a brief on the purpose and solicitation, as well as a statement on confidentiality.

The survey first sought to profile the experts based on qualifications and experience in ICT security. Level of responsibility is also gauged aimed at ranking the experts' importance and criticality weightings [2].

The actual questions were matrices with strategic assets as rows and 10 threat agents as columns. The answers involved 5 multiple choice drop-down answers per asset-threat-agent mapping.

Lastly, the strategic assets were mapped with perceived criticality (impact level) and the urgency with which these assets ought to be restored, in the event of a compromise or exploitation.

1.5. Outline

This introductory section dealt with the multi-attribute decision-making and its application to cyber-threats taxonomy, which is aimed at benchmarking cyber-assets of SMEs in developing economies. The problem resulting from deficit in taxonomy of threat agents concerning SMEs is underscored with some key questions raised that beg for redress.

The next section treats fuzzy aspects of multiple attributes decision-making techniques, using fuzzy similarity measures. This is followed by some empirical computations to rank the various threat agents, which are also discussed at length, in terms of characteristics and the possible impacts.

The paper concludes with some recommendations and outlook for future works.

II. FUZZY MULTI-ATTRIBUTE DECISION-MAKING (MADM)

Here, an approach is employed to rank the decision alternatives in multiple attribute decision-making problem of enlisting threats as perceived by the experts. The objective is that given ten (10) threat agents deduced from the main study as alternatives and evaluated in respect of six (6) susceptible cyber-assets, then fuzzy MADM techniques are used to rate them in the order of most-to-least.

It is noted herewith that this study chose to use fuzzy triangular numbers (FTNs), for simplicity and ease of computation. For instance, it can be showed that similar treatment with fuzzy trapezoidal numbers would yield similar results.

A. Fuzzy Similarity Measures

Fuzzy Similarity Measures is one of the basic concepts in human cognitive endeavors [25]. Fuzzy similarity measures finds applications in multi-attribute decision-making (MADM) such as "taxonomy, recognition, case-based reasoning" [25]. There are various aspects of fuzzy similarity measures, which are applied for variety and specific purposes [4] [26] etc.

Fuzzy similarity measures find applications in fuzzy ordering or ranking as well as fuzzy analysis of various risk

constructs. In this paper, fuzzy similarity measures are utilized in ranking various threat agents that confront SMEs in developing economies.

Beg & Ashraf [25] classified similarity measures into three (3) groups, namely:

i. Metric-based measures;
ii. Set-theoretic based measures; and
iii. Implicators based measures.

This paper dwells on an aspect of the set-theoretic based similarity measures. Indeed, set theoretic similarity measures come in two (2) types: crisp logic based and fuzzy logic based. Here again, this paper narrows down to the fuzzy logic similarity measures or fuzzy similarity measures, for brevity.

Similarity measures are sometimes referred to in literature as degrees or measures of similarity.

Generally, the fuzzy set theoretic provides the basis for generalizing the binary relations amongst any two (2) constructs [27].

Now, let the fuzzy linguistic variables be defined by the tuples $S = \{s_i : i = 1,2,.....,n\}$ such that $s_i < s_j$ iff i < j.

In this study, $S = \{s_1 = very - \min or,\ s_2 = \text{minor},\ s_3 = \text{important},\ s_4 = \text{vital},\ s_5 = \text{critical}\}$ and the experts are $E_i = \{E_1, E_2, ..., E_{14}\}$, that is the 14 respondents to the strategic interview survey.

From the empirical study (c.f. Table -1), expert E_1 is deemed the most important and assigned relative importance of $r_1 = 1$. Then, relative importance of the other experts, based on education attribute, are $r_2, r_3, ..., r_{10} = 0.8$ and $r_{11}, r_{12}, r_{13}, r_{14} = 0.6$.

Table 1: Expert Opinions Elicitation Dataset [2]

experts	Fuzzy Triangular Numbers(l)	Fuzzy Triangular Numbers (c')	Fuzzy Triangular Numbers(r')	relative importance	degree of importance	average agreement degree	relative agreement degree	consensus degree coefficients
E1	8	9	10	1	0.09	0.75	0.06	0.07
E2	6	7.5	9	0.8	0.08	0.88	0.08	0.08
E3	6	7.5	9	0.8	0.08	0.88	0.08	0.08
E4	6	7.5	9	0.8	0.08	0.88	0.08	0.08
E5	6	7.5	9	0.8	0.08	0.88	0.08	0.08
E6	6	7.5	9	0.8	0.08	0.88	0.08	0.08
E7	6	7.5	9	0.8	0.08	0.88	0.08	0.08
E8	6	7.5	9	0.8	0.08	0.88	0.08	0.08
E9	6	7.5	9	0.8	0.08	0.88	0.08	0.08
E10	6	7.5	9	0.8	0.08	0.88	0.08	0.08
E11	3	5	7	0.6	0.06	0.74	0.06	0.06
E12	3	5	7	0.6	0.06	0.74	0.06	0.06
E13	3	5	7	0.6	0.06	0.74	0.06	0.06
E14	3	5	7	0.6	0.06	0.74	0.06	0.06

Various degrees of importance can be computed from the equation

$$w_i = \frac{r_i}{\sum_{i=1}^{n} r_i}; \qquad [1\text{-}1]$$

For any given fuzzy sets $A = \{a_i\}$ and $B = \{b_i\}, \forall\ i = 1,2, ..., n$, the grade of similarity (or agreement degree) of the fuzzy relations is given by

$$S_{(A_i, B_i)} = \frac{\sum_i (a_i \wedge b_i)}{\sum_i (a_i \vee b_i)} \qquad [1\text{-}2]$$

Equation [1-2] is known as the min-max similarity method [28], and the fuzzy sets A and B are said to be approximately equal if and only if (iff), there exists a proximity measure, ε, [29] such that $S_{(R_i, R_j)} \equiv S_{(A,B)} \le \varepsilon.$ Generally, the fuzzy similarity measure estimates the degree of similarity between A and B. Similarity measures are metrics used to indicate the degree of similarity amongst constructs. For the two (2) fuzzy sets A and B, defined in the universe U, there exists a fuzzy relation such that: $S_{(A,B)} : \mu_A(x) * \mu_B(x) \to [0,1]$ is the fuzzy similarity measure if and only if the following axioms hold true:

i. $S_{(A,B)} = S_{(B,A)};\ \forall A, B \in U$
ii. $S_{(A,A)} = 1;\ \forall A \in U$
iii. $S_{(A,A')} = 0;\ \forall A \in U$
iv. $S_{(A,B)} \subseteq S_{(B,C)};\ \forall A \subseteq B \subseteq C$ and $A, B, C \in U$

Another useful method is that of Zeshui Xu [30] for similarity measure given by

$$S_{(R_i, R_j)} = 1 - \frac{|a_2 - a_1| + |b_2 - b_1| + |c_2 - c_1|}{8q} \qquad [1\text{-}3]$$

Where q = 3 for fuzzy triangular numbers and q = 4 for fuzzy trapezoidal numbers.

It is noted that $S_{(R_i, R_j)} \in [0\ 1]$ and $S_{(R_i, R_j)} \to 1$ implies that R_1 and R_2 are closer to each other. So $S_{(R_i, R_j)} = 1$ iff $R_1 = R_2$ and that also $S_{(R_i, R_j)} = S_{(R_j, R_i)}$

Assume that the fuzzy set $X = \{x_1, x_2, ..., x_n\}$ be the set of alternatives and $U = \{u_1, u_2, ..., u_m\}$ be the set of attributes. Then for a given degree of importance or weights vector $w = \{w_1, w_2, ..., w_m\};\ \forall\ w_i \ge 0;\ i = 1,2, ..., m.$ the linguistic decision matrix or agreement fuzzy matrix (AM) is computed as

$$AM_{mxn} = \begin{bmatrix} S_{11} & S_{12} & & S_{1n} \\ & & & \\ & & & \\ S_{m1} & S_{m2} & & S_{mn} \end{bmatrix} \quad [1\text{-}4]$$

or $AM_{mxn} \equiv (a_{ij})_{mxn}$ where $a_{ij} = [a_{ij}^a \;\; a_{ij}^b \;\; a_{ij}^c] \in S$ is the attribute value, which takes the form of a fuzzy triangular linguistic variable, given by the decision maker, for the alternative $x_j \in X$ with respect to the attribute $u_i \in U$. It follows that for a vector of attribute values $a_j = (a_{1j}, a_{2j}, ..., a_{mj})$ it corresponds with the alternative $x_j : j = 1,2,....., n$.

There exists an ideal point of attribute values, where $I_i = [I_i^a, I_i^b, I_i^c]$ such that $I_i^a = \max\{a_{ij}^a\},\ I_i^b = \max\{a_{ij}^b\},\ I_i^c = \max\{a_{ij}^c\}.$

Besides the min-max and Xu's fuzzy similarity measures, the following techniques have also been considered in evaluating the 10 threat agents in the taxonomy.

- Koczy & W-S Method [31]:

$$S_{(A_i,B_i)} = \frac{1}{1 + \sum_i |\mu_A(x_i) - \mu_B(x_i)|} = \left(1 + \sum_i |\mu_A(x_i) - \mu_B(x_i)| \right)^{-1} \quad [1\text{-}5]$$

- Guoshun & Yunsheng Method [32]

$$S_{(A_i,B_i)} = \frac{n - \sum_i |\mu_A(x_i) - \mu_B(x_i)|}{n + \sum_i |\mu_A(x_i) - \mu_B(x_i)|} \quad [1\text{-}6]$$

- Wang et al Method [33]

$$S_{(A_i,B_i)} = \frac{\sum_i |1 - (\mu_A(x_i) - \mu_B(x_i))|}{n} \quad [1\text{-}7]$$

- Hsieh & Chen Method [34]

$$S_{(A_i,B_i)} = \frac{1}{1 + d(A,B)} = \left(1 + d(A,B)\right)^{-1} \quad [1\text{-}8]$$

Where $d(A,B) = |P(A) - P(B)|$ and

$$P(A) = \frac{a_1 + 2a_2 + a_3}{4};\ P(B) = \frac{b_1 + 2b_2 + b_3}{4};$$

Using the empirical data on the 14 experts, 10 key cyber-security threat agents were identified and enlisted as the most common threat agents (vectors) of cyber-security compromises that affect the SMEs.

III. KEY THREATS EVALUATED

This sub-section deals with the actual computations leading to the ranking of threat agents in the taxonomy.

First the attributes are assigned fuzzy triangular numbers and weights vector based on the relative frequencies, $w = (0.10,\ 0.14, 0.24, 0.20, 0.15, 0.17)$.

The vector of alternatives for each threat agent is $X_j (j = 1,2,.....,10)$ are deduced. For example, $a_{11} = (4.5 \;\; 6.39 \;\; 7.78)$, $a_{21} = (5.43 \;\; 6.82 \;\; 8.21)$, $a_{31} = (6.93 \;\; 8.03 \;\; 9.14)$, etc.

From here, the ideal points are also determined $\hat{I} = (\hat{I}_1, \hat{I}_2, ..., \hat{I}_{10})$ where $\hat{I}_i = \max_j \{a_{ij}\}$. This implies that

$\hat{I}_1 = (6.93 \;\; 8.03 \;\; 9.14)$ and $\hat{I}_2 = (5.43 \;\; 6.72 \;\; 8.0)$ etc.

The similarity measures $\hat{Z}_j$ are computed for each of the attributes and then the overall values as well. Thus,

$$\hat{Z}_j = \sum w_i a_{ij}$$

$$where\ \text{i} = 1,2, ..., 6 \text{ and } \text{j} = 1, 2, ..., 10 \quad [1\text{-}9]$$

$$\Rightarrow \ \hat{Z}_1 = w_1 a_{11} \oplus w_2 a_{21} \oplus ..... \oplus w_6 a_{61}$$

Computing the overall or aggregated similarity measure as

$$\hat{Z}_* = w_1 \hat{I}_{11} \oplus w_2 \hat{I}_{21} \oplus ..... \oplus w_{10} \hat{I}_{10} \quad [1\text{-}10]$$

Where w_i is obtained from the relative importance.

$$\Rightarrow \ \hat{Z}_* = (6.12 \;\; 7.40 \;\; 8.68)$$

Table -2 below depicts the resulting computations from the above treatment :

Table 2: Resulting Computations

$\hat{Z}_i$	FTN	Ideal Point $\hat{I}_i$	FTN
$\hat{Z}_1$	(5.85 7.11 8.37)	$\hat{I}_1$	(6.93 8.03 9.14)
$\hat{Z}_2$	(4.74 6.10 7.46)	$\hat{I}_2$	(5.43 6.72 8.00)
$\hat{Z}_3$	(3.53 5.06 6.59)	$\hat{I}_3$	(4.93 6.40 7.86)
$\hat{Z}_4$	(5.77 7.03 8.30)	$\hat{I}_4$	(6.64 7.85 9.06)
$\hat{Z}_5$	(4.87 6.22 7.58)	$\hat{I}_5$	(5.78 7.10 8.42)
$\hat{Z}_6$	(5.51 6.80 8.10)	$\hat{I}_6$	(6.80 7.90 9.00)
$\hat{Z}_7$	(5.69 7.07 8.45)	$\hat{I}_7$	(6.40 7.65 8.90)
$\hat{Z}_8$	(4.25 5.76 7.27)	$\hat{I}_8$	(5.40 6.95 8.50)
$\hat{Z}_9$	(3.34 4.93 6.52)	$\hat{I}_9$	(4.90 6.40 7.90)
$\hat{Z}_{10}$	(6.91 8.07 9.23)	$\hat{I}_{10}$	(8.00 9.00 10.00)

The similarity degrees of the alternatives are subsequently determined as in the Table -3 below.

Table -3: Results of Similarity Measures on Threats Taxonomy

Similarity Measures $S_{(\hat{Z}_*,\hat{Z}_i)}$	Min-Max Method	Xu's Method	Hsieh & Chen	Koczy & W-S Method	Wang et al Method	Guoshum & Yunsheng
$S_{(\hat{Z}_*,\hat{Z}_1)}$	0.96	0.96	0.77	0.53	0.71	0.55
$S_{(\hat{Z}_*,\hat{Z}_2)}$	0.82	0.84	0.43	0.20	-0.30	-0.13
$S_{(\hat{Z}_*,\hat{Z}_3)}$	0.68	0.71	0.30	0.12	-1.34	-0.40
$S_{(\hat{Z}_*,\hat{Z}_4)}$	0.95	0.95	0.71	0.43	0.57	0.39
$S_{(\hat{Z}_*,\hat{Z}_5)}$	0.84	0.85	0.46	0.22	-0.18	-0.08
$S_{(\hat{Z}_*,\hat{Z}_6)}$	0.92	0.93	0.63	0.36	0.40	0.25
$S_{(\hat{Z}_*,\hat{Z}_7)}$	0.96	0.96	0.75	0.50	0.67	0.50
$S_{(\hat{Z}_*,\hat{Z}_8)}$	0.78	0.80	0.38	0.17	0.64	-0.24
$S_{(\hat{Z}_*,\hat{Z}_9)}$	0.67	0.69	0.29	0.12	-1.47	-0.42
$S_{(\hat{Z}_*,\hat{Z}_{10})}$	0.92	0.92	0.60	0.33	0.33	0.20

By definition of the fuzzy similarity measures, i.e. mapping into the unit interval [0,1], it is obvious that some of the methods do not strictly comply with the axioms. However, they all rank the alternatives in exact manner. Deducing from the above, the ranking of alternative threat agents are:

$$X_1 \approx X_7 > X_4 > X_6 \approx X_{10} > X_5 > X_2 > X_8 > X_3 > X_9$$

The taxonomy of threat agents as perceived by SMEs in developing economies are from the most likely attacks to the least, as follows:

i. Natural disasters
ii. Poor authentication
iii. Viruses and malware
iv. Hacking
v. No backup
vi. Spyware and adware
vii. Power failure
viii. Un-scanned attachments
ix. Spam
x. Social engineering.

IV. SMEs THREAT AGENTS DISCUSSED

This sub-section discusses the various threat agents that usually militate against most SMEs in developing economies.

i. Natural Disasters – here encompass any event considered as force majeure in legal parlance or business settings, including flood, earthquake, fire outbreak, excavations, etc. Karley [35] asserts that heavy rains in Accra, Ghana, for example, hamper economic activities and "telecommunications [infrastructure] are submerged in waters." The threat agent of floods in Ghana and Nigeria are perennial events (c.f. www.ghanadistricts.gov.gh alludes to the fact, citing "similar incidents were recorded in 1995, 1997 and 2001") [36].

CORDIS [37] in its project on "Advancing ICT for Disaster Recovery Management (DRM) in Africa" attests to the impact of natural disasters on ICT infrastructure, writing:

> "*Many developing countries in Africa are exposed to serious natural disaster risks and their need for an adequate ICT infrastructure supporting DRM is high. Unfortunately, access to ICT knowledge and affordable ICT systems is often lacking.*"

ii. Poor authentication – basically the authentication implemented in most networks or systems are the single-factor type, where username and a password dual is required before granting access to the end-user. This behooves enormous responsibility on the end-user to be cautious in choosing and administering his/her password. For systems or resources that are sensitive, it is incumbent upon the systems administrator to procure multi-factor authentication techniques, such as hardware (e.g. smartcard) and/or software (e.g. digital certificates & tokens) second-factor or third-factor (e.g. biometrics), which can ensure higher levels of security posture for the systems. Stronger passwords can be used with

extended strings coupled with alphanumeric and special characters [38].

An exploratory analysis of the type of authentication techniques used by the SMEs revealed that most of them (80%) used single-factor authentication or lesser mode, as depicted in the Figure -1.

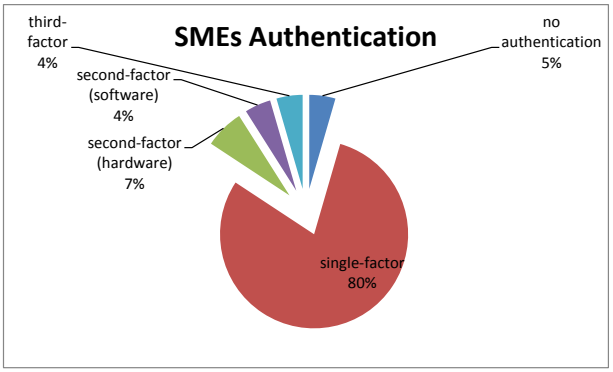

Figure - 1: SMEs Authentication Techniques

iii. Malware – is a term for malicious code or software, with the commonest forms as viruses and worms, which usually attacks computer systems or networks without the informed consent of the end-user [39]. Depending on the type and purposes of the malware, they may self-propagate (e.g. viruses), self-replicate (e.g. worms), self-discover (or has the ability to scan and discover other vulnerable assets, e.g. bots). The infection with malware may start by opening an attachment of an email. Some come through installation of software that have been compromised or are themselves malwares.

The OECD [40] best describes what a malware is:

"Malware can gain remote access to an information system, record and send data from that system to a third party without the user's permission or knowledge, conceal that the information system has been compromised, disable security measures, damage the information system, or otherwise affect the data and system integrity."

At the advent of computer malware, it was more of a nuisance to the end-user than a realized risk. With advancement in computer technologies, malwares have become very dangerous and disruptive due to their stealthy operations and sophistication of attacks.

Bots are typically scripts or programs with the capability to perform predefined functions repeatedly and automatically after being triggered intentionally or through a system infection [41]. Originally bots were intended as a useful program for repetitive automated and time consuming tasks, such as search engines, coordinating file transfers and online games, but they got exploited for malicious intentions.

For example, botnets have evolved as mere malware using Internet relay chat (IRC) protocols [42] to simulate distributed denial-of-service (DDoS) attacks, with great difficulty to trace and apprehend the botherder [43] [44].

The malware threat agents come in various ways including running an executable malware, through unpatched software vulnerabilities, backdoors, brute force attacks, emails, an unauthorized instant message, infected website, etc. Most malwares are transmitted like normal web traffic using regular ports, so as to evade firewalls and intrusion detection systems (IDS) [45].

iv. Hacking – is a process of breaking into one's system or decrypting a password, or by accessing one's network without authorization. Technically, any system can be hacked from anywhere via the Internet by exploiting identified vulnerabilities. Some of these vulnerabilities include a susceptible modem behind a firewall, weaknesses in TCP/IP and NetBIOS, exploiting an insecure wireless network, port scanning, packet sniffing, clickjacking, etc.

The erroneous notions of hackers looking for secrets, or "there's nothing attractive about one's network", have to be discarded. On the contrary, hackers take advantage of unprotected systems and may hack into systems for various reasons, including using infected systems as launch pads to attack others, gaining access to financial information, intellectual property, or corporate sensitive information, etc. [46].

v. No Backup – backup is a process of archiving data or making copies of programs or data unto separate storage media or additional resources for the purposes of being used for restoration or recovery, and usually keeping them out-of-site for security reasons. In the event of exploitation or attack, backups can be very useful to restore failed systems and/or restore corrupted data. Backups can greatly mitigate risks if the backups are robust and reliable [38]. Incidentally, most firms or end-users do not backup regularly (outdated copies) nor store off-site.

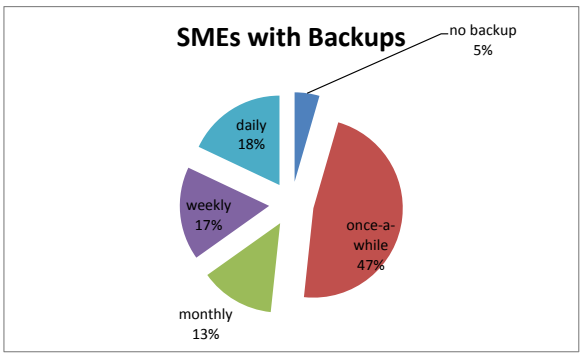

Figure - 2: SMEs Backup Trends

An exploratory analysis into the study revealed that 52% seldom backup, 13% backup monthly, 17% weekly

whilst 18% backup daily (see Figure -2), which compares with the mere 30% of Kenyan SMEs who backup regularly [47].

vi. Spyware (Adware) – spyware is a form of malware that spies on the user by stealthily collecting predefined user data for further actions [46]. They are usually installed unknowingly through web browsing or unprotected installations or downloads, especially as bundled freewares or peer-to-peer (P2P) applications. Typical examples of spyware are keystroke loggers, packet sniffers, instant messaging (IM) aggregators, etc. Adwares are not quite distinct from spyware except that they are usually used by some marketing firms (called sponsors) to collect information on users. The sponsors earn revenue through these adverts. They usually come in the form of pop-ups, "sponsored" freewares, toolbars, etc.

vii. Power failure – is the event of power supply outage to the ICT resources. It can be augmented with standby diesel engine generators (DEGs) or uninterruptible power supply (UPS) or solar cell power supplies to hold forth and supply power to essential resources in the event of outages. The augmented power supply are usually installed in functionally hot-standby mode, i.e. upon sensing commercial power failure, the standby units take-over automatically. In fact, due to the sensitive nature of the essential communications resources, the power supply is usually "sensitive" to power fluctuations and that any fluctuations outside the tolerance range are cut-off for smooth take-over by the conditioned UPS or other standby supply. For typical data centers or server farms, there are at least 2 different sources of UPS to ensure seamless switchovers [38].

viii. Un-scanned Attachment – this threat agent usually attacks when users open attachments to email messages without scanning them with up-to-date anti-virus software. In the corporate environments, most firms have policies dealing with email attachments. However, some end-users ignore or violate the policies and open unsuspecting attachments, e.g. "I Love You" (2005) or "Melissa" (1999) viruses.

This threat agent usually operates in concert with the last two agents, i.e. spam and social engineering.

ix. Spam is basically unsolicited email messages, usually received from unknown senders with "blank copied" numerous addressees. Spams could be spoofed as coming from legitimate or known sources and may have enticing content luring users to take certain detrimental actions [48]. In view of the growing awareness about spams and attachment threat agents, some spoof users with yet an enticing link. When users click on the link, the necessary scripts or programs are executed and the system may be infected or attacked or used as launch pads.

x. Social engineering is the "practice" of manipulating or luring end-users to divulge confidential information by appealing to their sense of social norms, with the aim to gain access to one's system [46]. This threat agent exploits the vulnerability of end-users, e.g. receptionists, to solicit access credentials. The social engineer exploits and leverages on pre-existing trusted relationship amongst a victim and the assumed entity, to lure the victim to take some detrimental actions [49]. Some examples of social engineering are information gathered via telephone calls purporting to be a system administrator, or a consultant or a visitor asking to use a corporate computer, etc.

The imprecision in the cyber-threats and associated likelihood of maturity is represented by fuzzy numbers. Various fuzzy similarity measures are in literature, however, this paper only reviewed those few measures that easily give credence to the threat agents taxonomy. It suffices to say that some of the methods would have ranked the threats differently, but the essence for a standardized cyber-threats taxonomy remains pertinent.

V. CONCLUSIONS

Advancement in ICTs and globalization have motivated SMEs to embrace the Internet as vital business tools, for operations and business communications. Closely associated with these enormous opportunities are vulnerabilities and threats, which pose serious risks to all businesses, especially SMEs and more so if located in developing or emerging economies.

Also confronting today's tech-savvy business managers are plethora of operational and strategic decisions. Amongst the strategic aspects of business decisions are the challenges of cyber-security and information assurance. New and innovative security challenges confront the SMEs on a daily basis, thus exploiting most "zero-day" vulnerabilities. This results in various losses to the SMEs, even with the possibility of business closure. SMEs ought to ensure that their networks and systems are both available and secured. The decision scenarios are mainly subjective and are usually fraught with lots of uncertainties.

Cognizant of the above, any proposed solutions must necessarily be holistic and account for the intrinsic nature of the decision attributes and alternatives. Fuzzy multi-attributes decision-making techniques are suitable for the analysis and evaluation of threat agents taxonomy.

This study has been about being able to identify some key threats and to prefer proactive mitigation measures to deal with them. This study identified the ten (10) top-most threats that commonly exploit SMEs in developing economies. Again, fuzzy similarity measures were applied with multi-attribute decision-making techniques to benchmark the taxonomy of threat agents. These threat agents are natural disasters that are perennial in developing economies, poor authentication

methods, power outages and failure – another perennial problem in developing economies, viruses, hacking, no backups, un-scanned attachments, spamming, spywares, and social engineering due to apparent gullibility of most cultures in developing economies.

These simple approaches employed in identifying and creating the taxonomy are geared towards assisting SMEs to have some base metrics for referencing in risk management and information assurance.

Accurate identification of critical assets can lead to proactive detection and preventive measures that ultimately can mitigate the associated risks.

In conclusion, the novel approach of evaluating cyber-threats based on intuitive, subjective and holistic assessment aimed at creating a taxonomy to fill the void created by the lack of standardized lists of threats. At least, SMEs can have some empirical basis of cyber-threats to benchmark their business and security performance metrics, rather than relying upon the usual "TV news effect" of most-publicized compromises with disproportionate mitigation measures.

Future research work will be focused on exploring other fuzzy relational measures, the differences resulting from other fuzzy similarity measures and their axioms.

REFERENCES

[1] Prince, Daniel & Nick King, "Small Businesses: Cyber-security Survey 2012," Security Lancaster & Lancaster University, UK, 2012.

[2] E. O. Yeboah-Boateng, "Cyber-Security Challenges with SMEs in Developing Economies: Issues of Confidentiality, Integrity & Availablity (CIA)," center for Communications, Media & Information technologies (CMI), Aalborg University, Copengahen, 2012.

[3] Sincich, Terry, James MClave & William Mendenhall, A First Course in Statistics, 9th ed., Prentice Hall, 2005.

[4] Anisseh, Mohammed & Rosnah bt. Mohd Yussuf, "A Fuzzy Group Decision Making Model for Multiple Criteria based on Borda Count," *International Journal of the Physical Sciences*, vol. 6, no. 3, pp. 425-433, 2011.

[5] B. M. Ayyub, Elicitation of Expert Opinions for Uncertainty & Risks, CRC Press LLC, 2001.

[6] L. Zadeh, "Fuzzy Sets as a Basis for a Theory of Possibility," *Fuzzy Sets & Systems*, vol. 1, pp. 3-28, 1978.

[7] S.-J. Chuu, "Group Decision-Making Model using Fuzzy Multiple Attributes Analysis for the Evaluation of Advanced Manufacturing Technology," *Fuzzy Sets & Systems*, vol. 160, no. 5, pp. 586-602, 2009.

[8] S. K. Katsikas, "Risk Management," in *Computer & Information Security Handbook*, Morgan-Kaufmann, Inc., 2009, pp. 605-625.

[9] K. M. Shaurette, "The Building Blocks of Information Security," in *Information Security Management Handbook*, 2002.

[10] A. Deaton, "Savings in Developing Countries: Theory & Review," in *Proceedings of the World Bank Annual Conference on Developing Countries, 1989.*, 1990.

[11] Walsham, Geoff & Sundeep Sahay, "Research on Information Systems in Developing Countries: Current Landscape & Future Prospects," *Information Technology for Development*, 2005.

[12] Ellefsen, I.D. & S.H. von Solms, *Framework for Cyber Security Structure in Developing Countries*, University of Johannesburg, 2012.

[13] International Telecommunications Union (ITU), "International Multilateral Partnership Against Cyber Threats (IMPACT)," ITU, 2011.

[14] International Telecommunications Union (ITU), "Guide to Cyber-security for Developing Countries," ITU, 2007.

[15] P. Julien, The State of the Art in Small Business & Enterprenuership, Ashgate, Aldershot, 1998.

[16] B. Planque, "La PME Innovatrice: Quel est le role du milieu local?," *Revue Internationale PME*, vol. 1, no. 2, pp. 177-191, 1988.

[17] L. Pierre, "The Wall Street Networks," 2008.

[18] Sharma, Kunal, Amarjeet Singh & Ved Prakash, "SMEs & Cyber-security Threats in e-Commerce," vol. 39, no. 5-6, pp. 1-49, 2009.

[19] Abouzakhar, N. et al, "An Intelligent approach to Prevent Distributed Systems Attack," vol. 10, no. 5, pp. 203-209, 2002.

[20] M. Dondo, "A Fuzzy Risk Calculations Approach for a Network Vulnerability," 2007.

[21] D. Denning, "Cyber-Security as an Emergent Infrastructure," in *Bombs & Bandwidth: The Emerging Relationship between IT & Security*, The New Press, 2003.

[22] J. Mallery, "Building a Secure Organization," in *Computer & Information Security Handbook*, Morgan-Kaufmann, Inc., 2009, pp. 3-22.

[23] T. Casey, "Threat Agent Library Helps Identify Information Security Risks," Intel Information Techonology, 2007.

[24] E. O. Yeboah-Boateng, "Using Fuzzy Cognitive Maps (FCMs) To Evaluate The Vulnerabilities With ICT Assets Disposal Policies," *International Journal of Electrical & Computer Sciences IJECS-IJENS*, vol. 12, no. 5, pp. 20-31, October 2012.

[25] Beg, Ismat & Samina Ashraf, "Similarity Measures of Fuzzy Sets," *Applications & Computational Mathematics*, vol. 8, no. 2, pp. 192-202, 2009.

[26] Deng, Yong, Bing Yi Kang, Ya Juan Zhang, Xin Yang Deng & Hai Xin Zhang, "A Modified Similarity Measure of Generalized Fuzzy Numbers," in *Chinese Control & Decision Conference (CCDC)*, 2011.

[27] Lui, W.N. & J.T. Yao & Y.Y. Yao, "Constructive Fuzzy Sets with Similarity Semantics," in *North American Fuzzy Information Processing Society (NAFIPS)*, 2005.

[28] Hsu, Hsi-Mei & Chen-Tung Chen, "Aggregation of Fuzzy Opinions Under Group Decision Making," *Fuzzy Sets & Systems*, vol. 79, pp. 279-285, 1996.

[29] Pappis, Costas & Nikos Karacapilidis, "A Comparative Assessment of Measures of Similarity of Fuzzy Values," *Fuzzy Sets & Systems*, vol. 56, pp. 171-174, 1993.

[30] Z. Xu, "An Approach Based on Similarity Measure to Multiple Attribute Decision Making with Trapezoid Fuzzy Linguistic Variables," in *Fuzzy Systems & Knowledge Discovery - Lecture Notes in Artificial Intelligence*, vol. 3613, Springer, 2005, pp. 110-117.

[31] Koczy, L.T. & T. Domonko, Fuzzy Systems (Fuzzy Rendszrek), Budapest, Hungary: Typotex, 2000.

[32] Guoshun, Huang & Liu Yunsheng, "New Subsethood Measures and Similarity Measures of Fuzzy Sets," in *International Conference on Communications, Circuits & Systems*, 2005.

[33] Wang, Ying-Ming, Jian-Bo Yang, Dong-Ling Xu & Kwai-Sang Chin, "On The Centriods of Fuzzy Numbers," *Fuzzy Sets & Systems*, vol. 157, pp. 919-926, 2006.

[34] Hsieh, C.H. & S.H. Chen, "Similarity of Generalized Fuzzy Numbers witrh Graded Mean Integration Representation," in *8th International Fuzzy Systems Association World Congress*, Taipei, Taiwan, 1999.

[35] N. K. Karley, "Flooding & Physical Planning in Urban Areas in West Africa: Situational Analysis of Accra, Ghana," *Theoretical & Empirical Researches in Urban Management*, pp. 25-41, 2009.

[36] I. Adelekan, "Vulnerability of Poor Urban Coastal Communities to

Flooding in Lagos, Nigeria," *Envrionment & Urbanization*, vol. 22, no. 2, pp. 433-450, 2010.

[37] CORDIS, "Advancing ICT for Disaster Recovery Maanagement in Africa," Community Research & Development Information Service, Brussels, 2010.

[38] B. Mansoor, "Intranet Security," in *Computer & Information Security Handbook*, Morgan-Kaufmann, Inc., 2009, pp. 133-148.

[39] A. Caballero, "Information Security Essentials for IT Managers: Protecting Mission-Critical Systems," in *Computer & Information Security Handbook*, Morgan-Kaufmann, Inc., 2009, pp. 225-253.

[40] OECD, "Malicious Software (Malware): A Security Threat to the Internet Economy," Organization for Economic Cooperation & Development, 2009.

[41] Bandy, M.T. et al, "Study of Botnets & their Threats to Internet Security," *Working Papers on Information Security*, 2009.

[42] IETF, "RFC 2812 & ISON," 2001. [Online]. Available: www.irc.org/mla/ircd/2001/.

[43] C. Day, "Intrusion Prevention & Detection Systems," in *Computer & Information Security Handbook*, Morgan-Kaufmann, 2009, pp. 293-306.

[44] Schiller, C., Seth Fogie, Colby DeRodeff & Michael Gregg, InfoSecurity 2008: Threat Analysis, Syngress, 2007.

[45] Georgia Tech, "Emerging Cyber Threats Report for 2009," Information Security Center, 2008.

[46] Young, Susan & Dave Aitel, The Hacker's Handbook - Strategies for Breaking Into and Defending Networks, CRC Press, 2007.

[47] J. O. Ogalo, "The Impact of Information Systems Security Policies & Controls on Firm Operation Enhancement for Kenyan SMEs," *Prime Journal of Business Administration & Management*, vol. 2, no. 6, pp. 573-781, June 2012.

[48] Wang, Xinyuan & Daniel Ramsbrock, "The Botnet Problem," in *Computer & Information Security Handbook*, Morgan-Kaufmann, 2009, pp. 119-132.

[49] Jacobsson, Markus & Alex Tsow, "Identity Theft," in *Computer & Information Security Handbook*, Morgan-Kaufmann, 2009, pp. 519-549.

[50] ITU, "A Comparative Analysis of Cyber-security Initiatives Worldwide," International Telecommunications Union (ITU), 2005.

[51] Warner, *International Journal of Cyber Criminology*, 2011.

BIOGRAPHIES

Ezer Osei Yeboah-Boateng is a Ph.D. candidate in Cyber-Security at the center for Communications, Media & Information technologies (CMI), Aalborg University in Copenhagen, Denmark. Ezer holds an M.S. degree in Telecommunications (Magna cum Laude), with concentrations in Wireless Network Security and digital signal processing (DSP), from the Stratford University, Virginia, USA, and a B.Sc. (Honors) in Electrical & Electronic Engineering from the University of Science & Technology (U.S.T.) in Kumasi, Ghana.

Ezer is a professional ICT Specialist with a strong background in cyber-security, business development, knowledge management and capabilities to develop market-oriented strategies aimed at promoting growth and market share. He is an Executive with more than 20 years of domestic and global experience conceptualizing ideas, seizing opportunities, building operations, leading highly successful new business development initiatives and ventures.